UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/057,914	01/29/2002	Jens-Peter Redlich	A7995	3714

7590 10/01/2008

SUGHRUE MION, PLLC
2100 Pennsylvania Avenue NW
Washington, DC 20037-3213

EXAMINER	
PATEL, CHIRAG R	
ART UNIT	PAPER NUMBER
2141	
MAIL DATE	DELIVERY MODE
10/01/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 10/057,914
Filing Date: January 29, 2002
Appellant(s): REDLICH ET AL.

Redlich et al.
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed June 2, 2002 appealing from the Office action mailed October 25, 2007.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is incorrect.

No amendment after final has been filed. Claim 35 was previously cancelled in the prior amendments.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

6,226,677	Slemmer	5-2001

6,751,729	Giniger	6-2004
6,243,450	Jansen	06-2001
6,957,276	Bahl	10-2005

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-22, 24-25, 28-32, 36-37, and 39-40 are rejected under 35 U.S.C. 103(a) as being unpatentable over Slemmer (US 6,226,677) in view of Giniger et al. – hereinafter Giniger (US 6,751,729).

As per claim 1, Slemmer discloses a method for performing mutual authentication and authorization of a user's terminal device (U) and an Internet Service Provider (P) in order to establish secure communication between the terminal (U) and a trusted network element (T) to the Internet via an untrusted access station (A) comprising:

establishing an association between a terminal (U) and an untrusted access station (A); (Col 3 line 65 – Col 4 line 18, Figure 1: items 120, 130)

transmitting an ISP authentication packet from terminal (U) to ISP (P) via the untrusted access station (A); (Col 6 line 55 – Col 7 line 52)

sending a user authentication packet from said ISP (P) to said terminal (U) via said untrusted access station (A); (Col 6 line 55 – Col 7 line 52)

wherein a connection is established between the terminal the ISP for trusted network services without providing the terminal with direct access to the internet. (Col 6 line 55- Col 7 line 52)

Slemmer fails to disclose upon authentication of said terminal (U) and said ISP (P), said ISP performs the following: generating a session key;

distributing said session key to said terminal (U) and a trusted network element (T), wherein said session key is used to encrypt traffic between the terminal (U) and the trusted network element (T);

establishing a secure tunnel such that the terminal (U) may communicate with the Internet via said trusted network element (T); wherein said secure tunnel emulates a physical link between the terminal (U) and the trusted network element (T) such that traffic transmitted between the terminal (U) and said Internet via said trusted network element (T) is secure from modification or eavesdropping by said third party access station (A).

Giniger discloses upon authentication of said terminal (U) and said ISP (P), said ISP performs the following: generating a session key; (Col 15 lines 16-22)

distributing said session key to said terminal (U) and a trusted network element (T), wherein said session key is used to encrypt traffic between the terminal (U) and the trusted network element (T); (Col 15 lines 16-22)

establishing a secure tunnel such that the terminal (U) may communicate with the Internet via said trusted network element (T); wherein said secure tunnel emulates a physical link between the terminal (U) and the trusted network element (T) (Col 11 lines 55-58)

such that traffic transmitted between the terminal (U) and said Internet via said trusted network element (T) is secure from modification or eavesdropping by said third party access station (A). (Col 6 lines 14-22, Col 12 lines 14-22)

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to disclose generating a session key; distributing said session key to said terminal (U) and a trusted network element (T), wherein said session key is used to encrypt traffic between the terminal (U) and the trusted network element (T); such that traffic transmitted between the terminal (U) and said Internet via said trusted network element (T) is secure from modification or eavesdropping by said third party access station (A) in the disclosure of Slemmer. The motivation for doing do would have been to provide comprehensive security to guarantee the safe transmission of mission critical data over public networks. (Col 6 lines 14-22).

As per claim 2, Slemmer/ Giniger disclose the method of claim 1. Slemmer discloses the method for performing mutual authentication and

authorization of a terminal (U) and an Internet Service Provider (P) in order to establish a secure tunnel between the terminal (U) and a trusted network element to the Internet (T) via an untrusted access station (A) of claim 1, wherein the ISP (P) authentication packet contains an authentication challenge (CH_U) from terminal (U) to ISP (P) to authenticate the identity of ISP (P). (Col 6 line 55- Col 7 line 52)

As per claim 3, Slemmer / Giniger disclose the method for for performing mutual authentication and authorization of a terminal (U) and an Intemet Service Provider (P) in order to establish a secure tunnel between the terminal (U) and a trusted network element to the Internet (T) via an untrusted access station (A) of claim 1. Slemmer discloses wherein the user authentication packet contains an authentication challenge (CH_P) from ISP (P) to the terminal (U) to authenticate the identity of user (U). (Col 6 line 55- Col 7 line 52)

As per claim 4, Slemmer discloses a method for providing public access to IP-based networks via an untrusted infrastructure having untrusted access points comprising:

establishing a connection between an IP-device (U) and said untrusted access point (A), (Col 3 line 65 – Col 4 line 18, Figure 1: items 120, 130)

transmitting an ISP authentication request from said IP device (U) to an intemet service provider (P) affiliated with said IP device (U), wherein said authentication request is transmitted through said untrusted access point (A) affiliated with said untrusted third party owned infrastructure; (Col 6 line 55 – Col 7 line 52, Col 8 line 35-48; an embodiment of the control system implemented for a multi-unit property (e.g., a hotel, an apartment or the like)

transmitting a user authentication request from said ISP (P) to said IP device (U) to determine whether said IP device (U) is a valid user affiliated with said ISP (P), wherein said authentication request is transmitted through said untrusted access point (A) affiliated with said untrusted third party owned infrastructure; (Col 6 line 55 – Col 7 line 52)

wherein a connection is established between the terminal and the ISP for trusted network services without providing the terminal with direct access to the Internet. (Col 6 line 55- Col 7 line 52)

Slemmer fails to disclose when said ISP (P) authentication request and said user authentication requests is affirmative, said ISP (P): generates a key session for encrypting data packets; and distributes said session key to said IP device (U) and a trusted node (T), wherein said session key is used to encrypt data transmitted between said IP device (U) and said trusted node (T); establishing a secure tunnel as said session key is used to encrypt data packets transmitted between said IP device (U) and said trusted node (T), such that said data packets transmitted between said IP device (U) and an Internet via the untrusted access station (A) are

protected from modification and manipulation by said untrusted access station (A) in said secure tunnel, wherein an IP address is dynamically allocated to said IP device.

Giniger discloses generates a key session for encrypting data packets; and distributes said session key to said IP device (U) and a trusted node (T), (Col 15 lines 16-22)

wherein said session key is used to encrypt data transmitted between said IP device (U) and said trusted node (T); establishing a secure tunnel as said session key is used to encrypt data packets transmitted between said IP device (U) and said trusted node (T), (Col 11 lines 55-58)

such that said data packets transmitted between said IP device (U) and an Internet via the untrusted access station (A) are protected from modification and manipulation by said untrusted access station (A) in said secure tunnel, (Col 6 lines 14-22, Col 12 lines 14-22)

wherein an IP address is dynamically allocated to said IP device. (Col 11line 59 – Col 12 line 2)

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to disclose when said ISP (P) authentication request and said user authentication requests is affirmative, said ISP (P): generates a key session for encrypting data packets; and distributes said session key to said IP device (U) and a trusted node (T), wherein said session key is used to encrypt data transmitted between said IP device (U) and said trusted node (T); establishing a secure tunnel as said session key is used to encrypt data packets transmitted between said IP device (U) and

said trusted node (T), such that said data packets transmitted between said IP device (U) and an Internet via the untrusted access station (A) are protected from modification and manipulation by said untrusted access station (A) in said secure tunnel, wherein an IP address is dynamically allocated to said IP device in the disclosure of Slemmer. The motivation for doing do would have been to provide comprehensive security to guarantee the safe transmission of mission critical data over public networks. (Col 6 lines 14-22).

As per claim 5, Slemmer discloses a method for providing public access to IP-based networks through a third party owned, untrusted infrastructure having untrusted access stations (A) comprising:

establishing a connection between an IP-device (U) and said access station (A), (Col 3 line 65 – Col 4 line 18, Figure 1: items 120, 130)

sending an ISP authentication request to said internet service provider (P) affiliated with said IP device (U) requesting to validate the authenticity of the ISP (P); sending a user authentication request from said ISP (P) to said IP device (U) to validate whether said IP device (U) has a service agreement with said ISP (P); (Col 6 line 55 – Col 7 line 52

wherein a connection is established between the terminal and the ISP for trusted network services without providing the terminal with direct access to the Internet. (Col 6 line 55 – Col 7 line 52)

Slemmer fails to disclose upon affirmative authentication of said ISP (P) and said IP device (U); establishing a trusted connection between said IP device (U) and a

trusted network element (T), wherein a secure tunnel allows the ISP (P) to dynamically obtain control of resource in said untrusted third party owned access station (A) in order to provide the IP device (U) with prescribed for services, wherein an IP address is dynamically allocated to said IP device (U).

Giniger discloses upon affirmative authentication of said ISP (P) and said IP device (U); establishing a trusted connection between said IP device (U) and a trusted network element (T), wherein a secure tunnel allows the ISP (P) to dynamically obtain control of resource in said untrusted third party owned access station (A) in order to provide the IP device (U) with prescribed for services, (Col 11 lines 55-58, Col 15 lines lines 16-22)

wherein an IP address is dynamically allocated to said IP device (U); (Col 11line 59 – Col 12 line 2)

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to disclose upon affirmative authentication of said ISP (P) and said IP device (U); establishing a trusted connection between said IP device (U) and a trusted network element (T), wherein a secure tunnel allows the ISP (P) to dynamically obtain control of resource in said untrusted third party owned access station (A) in order to provide the IP device (U) with prescribed for services, wherein an IP address is dynamically allocated to said IP device (U) in the disclosure of Slemmer. The motivation for doing do would have been to guarantee the safe transmission of mission critical data over public networks. (Col 6 lines 14-22)

As per claim 6, Slemmer discloses a method of establishing secure communication between a terminal (U), the Internet Service Provider (P) affiliated with that terminal and the Internet over a third party owned untrusted access station (A) comprising:

establishing a connection between the terminal (U) and said access station (A); sending an ISP authentication request to said internet service provider (P) affiliated with said terminal (U); (Col 3 line 65 – Col 4 line 18, Figure 1: items 120, 130)

sending a user authentication request from said ISP (P) to said terminal (U); (Col 6 line 55 – Col 7 line 52)

wherein a connection is established between the terminal and the ISP for trusted network services without providing the terminal with direct access to the Internet. (Col 6 line 55 – Col 7 line 52)

Slemmer fails to disclose upon affirmative authentication of said ISP (P) and said terminal (U): establishing a trusted connection between said IP device (U) and a trusted network element (T), wherein a secure tunnel allows the ISP (P) to dynamically obtain control of resource in said untrusted access station (A) in order to provide the IP device (U) with prescribed for services.

Giniger discloses upon affirmative authentication of said ISP (P) and said terminal (U): establishing a trusted connection between said IP device (U) and a trusted network element (T), wherein a secure tunnel allows the ISP (P) to dynamically obtain control of resource in said untrusted access station (A) in order to provide the IP device (U) with prescribed for services. (Col 11 lines 55-58, Col 15 lines lines 16-22)

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to disclose discloses upon affirmative authentication of said ISP (P) and said terminal (U): establishing a trusted connection between said IP device (U) and a trusted network element (T), wherein a secure tunnel allows the ISP (P) to dynamically obtain control of resource in said untrusted access station (A) in order to provide the IP device (U) with prescribed for services in the disclosure of Giniger. The motivation for doing do would have been to guarantee the safe transmission of mission critical data over public networks. (Col 6 lines 14-22).

As per claim 7, Slemmer / Giniger disclose a method of establishing secure communication between a terminal (U), the Internet Service Provider (P) affiliated with that terminal and the Internet over an untrusted access station (A) of claim 6. Slemmer discloses wherein the ISP authentication request contains an authentication challenge (CH_U) from terminal (U) to ISP (P) to authenticate the identity of ISP (P). (Col 6 line 55 – Col 7 line 52)

As per claim 8, Slemmer / Giniger disclose a method of establishing secure communication between a terminal (U), the Internet Service Provider (P) affiliated with that terminal and the Internet over an untrusted access station (A) of claim 6. Slemmer discloses wherein the user authentication request contains an authentication challenge (CH_IP) from ISP (P) to the terminal (U) to authenticate the identity of terminal (U) as having subscribed to said ISP (P) for services. (Col 6 line 55 – Col 7 line 52)

As per claims 9-14, and 37, please see the discussion under claim 1 as similar logic applies.

As per claim 15, Slemmer / Giniger disclose a method of establishing secure communication between a terminal (U), the Internet Service Provider (P) affiliated with that terminal and the Internet over an untrusted access station (A) of claim 6. Slemmer fails to disclose a time out is distributed to the trusted node (T) and terminal (U) upon the establishment of a secure tunnel. Giniger discloses a time out is distributed to the trusted node (T) and terminal (U) upon the establishment of a secure tunnel. (Col 12 lines 9-13) At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to disclose a time out is distributed to the trusted node (T) and terminal (U) upon the establishment of a secure tunnel in the disclosure of Slemmer. The motivation for doing do would have been to guarantee the safe transmission of mission critical data over public networks. (Col 6 lines 14-22).

As per claim 16, Slemmer / Giniger discloses a method of establishing secure communication between a terminal (U), the Internet Service Provider (P) affiliated with that terminal and the Internet over an untrusted access station (A) of claim 15. Slemmer fails to disclose wherein the timeout value is set to a predetermined time period, wherein if the secure tunnel is active for a time period equal to the timeout value, the secure tunnel will expire and the resources utilized for the secure tunnel will be

releases. Giniger discloses wherein the timeout value is set to a predetermined time period, wherein if the secure tunnel is active for a time period equal to the timeout value, the secure tunnel will expire and the resources utilized for the secure tunnel will be releases (Col 6 lines 23-27, Col 12 lines 9-13, Col 17 lines 28-34)

As per claims 17-22, please see the discussion under claim 1 as similar logic applies.

As per claims 24-25, 28-30, and 40, please see the discussion under claim 4 as similar logic applies.

As per claim 31, Slemmer / Giniger disclose a method of establishing secure communication between a terminal (U), the Internet Service Provider (P) affiliated with that terminal and the Internet over an untrusted access station (A) of claim 6, wherein the untrusted access stations (A) is compatible with at least one wireless transmission standard including WLAN (IEEE 802.11), BlueTooth (IEEE 802.15), or HiperLan. (Col 4 line 64 – Col 5 line 14)

As per claim 32, Slemmer / Giniger disclose a method of establishing secure communication between a terminal (U), the Internet Service Provider (P) affiliated with that terminal and the Internet over an untrusted access station (A) of claim 6. Slemmer discloses wherein the terminal (U) is a mobile device. (Col 6 line 58 – Col 7 line 48)

As per claim 36, Slemmer discloses a method of operating an untrusted access station deployed so as to provide a local network with access to a wide area network, the method comprising:

an untrusted access station receiving a request from a terminal to access trusted network services; (Col 3 line 65 – Col 4 line 18, Figure 1: items 120, 130)

without providing the terminal with direct access to the wide area network, establishing a connection between the terminal and an authentication server for trusted network services performing authentication of the terminal with the authentication server for the trusted network services; (Col 6 line 55 – Col 7 line 52)

Slemmer fails to disclose allowing the terminal to establish a secure channel to trusted network services across the wide area network only if the authentication succeeds. Giniger discloses allowing the terminal to establish a secure channel to trusted network services across the wide area network only if the authentication succeeds. (Col 11 lines 55-58, Col 15 lines 16-22) At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to disclose allowing the terminal to establish a secure channel to trusted network services across the wide area network only if the authentication succeeds in the disclosure of Slemmer. The motivation for doing do would have been to provide comprehensive security to guarantee the safe transmission of mission critical data over public networks. (Col 6 lines 14-22).

As per claim 39, Slemmer / Giniger disclose the method of claim 36. Slemmer disclose wherein the networks are Internet Network Protocol networks. (Col 2 lines 25-44)

Claims 23, 26-27, 34, and 38 are rejected under 35 U.S.C. 103(a) as being unpatentable over Slemmer (US 6,226,677) / Giniger (US 6,751,729) further in view of Jansen et al. – hereinafter Jansen (US 6,243,450)

As per claims 23, 26-27, and 38, Slemmer / Giniger disclose a method of establishing secure communication between a terminal (U), the Internet Service Provider (P) affiliated with that terminal and the Internet over an untrusted access station (A) of claim 6. Slemmer fails to disclose wherein the ISP (P) provides an accounting of time to the untrusted access station (A) for resources utilized by the terminal (U). Jansen discloses wherein the ISP (P) provides an accounting of time to the untrusted access station (A) for resources utilized by the terminal (U). (Col 2 lines 35-42) At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to disclose wherein the ISP (P) provides an accounting of time to the untrusted access station (A) for resources utilized by the terminal (U). Jansen discloses wherein the ISP (P) provides an accounting of time to the untrusted access station (A) for resources utilized by the terminal (U) in the disclosure of Slemmer. The motivation for doing do would have been to provide a pay-per use billing to end-users of public access services available through an Internet-accessible kiosk or terminal. (Col 1

lines 19-25)

As per claim 34, Slemmer / Giniger discloses a method of establishing secure communication between a terminal (U), the Internet Service Provider (P) affiliated with that terminal and the Internet over an untrusted access station (A) of claim 6. Slemmer fails to disclose wherein the untrusted access station (A) assigns an local unique identification (LUID) to the terminal (U) in order to facilitate matching the terminal with data packets when the untrusted access station (A) is simultaneously serving multiple terminals (U). Jansen discloses wherein the untrusted access station (A) assigns an local unique identification (LUID) to the terminal (U) in order to facilitate matching the terminal with data packets when the untrusted access station (A) is simultaneously serving multiple terminals (U). (Col 9 lines 21-35) At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to disclose wherein the untrusted access station (A) assigns an local unique identification (LUID) to the terminal (U) in order to facilitate matching the terminal with data packets when the untrusted access station (A) is simultaneously serving multiple terminals (U) in the disclosure of Slemmer. The motivation for doing do would have been to provide a pay-per use billing to end-users of public access services available through an Internet-accessible kiosk or terminal. (Col 1 lines 19-25)

Claims 33 and 41 are rejected under 35 U.S.C. 103(a) as being unpatentable over Slemmer (US 6,226,677) / Giniger (US 6,751,729) further in view of Bahl (US 6,957,276).

As per claims 33 and 41, Slemmer / Giniger discloses a method of establishing secure communication between a terminal (U), the Internet Service Provider (P) affiliated with that terminal and the Internet over an untrusted access station (A) of claim 6. Slemmer fails to disclose wherein the terminal (U) recognizes a compatible access point by broadcasting a dynamic host configuration protocol (DHCP) request and receiving a "magic" DHCP response from the untrusted access station (A). Bahl discloses wherein the terminal (U) recognizes a compatible access point by broadcasting a dynamic host configuration protocol (DHCP) request and receiving a "magic" DHCP response from the untrusted access station (A). (Col 3 lines 8-27) At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to disclose wherein the terminal (U) recognizes a compatible access point by broadcasting a dynamic host configuration protocol (DHCP) request and receiving a "magic" DHCP response from the untrusted access station (A) in the disclosure of Reference A. The motivation for doing do would have been to reclaim a permanent or static IP address from a machine without having to physically go to the machine. (Col 2 line 65 – Col 3 line 7)

(10) Response to Argument

1. Applicant argues "General Remarks"

Response to 1.)

Examiner will point out below that the teachings of the prior art , see (8) Evidence Relied Upon, in the non-final office action dated October 22, 2007 clearly reads on recited claim language.

2. Applicant argues "Claims 1-22, 24-25, 28-32, 36-37 and 39-40 are not obvious over the combined teachings of Slemmer and Giniger.

Response to 2.)

Examiner has interpreted per Figure 1: items 120 in Slemmer as the user's terminal device (U) and Figure 1: item 130 as the untrusted access station (A). Slemmer discloses per an ISP connection and how Fig. 1: item 120 is used for internet access per Col 6 line 55 – Col 7 line 52, "With reference to FIG. 3, a user plugs in a laptop and runs the browser in step 300. The user's default web page is a first URL home.browserid.com/Index.htm. The user's laptop (user machine 120) attempts to connect to port 80 of home.browserid.com in step 304. The server 130 redirects this request to the forced proxying or control program. The control program determines that this is the first time it has seen this user machine 120. The control program returns a HTTP redirect message sending the user machine 120 to a second URL at www.login.com in step 308. The user's laptop receives this message and now tries to fetch www.login.com by attempting to connect to port 80 of www.login.com in step 312.

The server 130 redirects this request to the control program. The control program recognizes the second URL at www.login.com."

Additionally, Slemmer discloses connection to Internet Service Provider per Col 6 line 55 - Col 7 line 52, "The control program disables forced proxying for this user machine IP address. The user machine 120 displays a "logging you in . . . " message for five seconds and then the www.lodgenet.com home page is displayed in step 336. The operator of this user machine 120 can then begin to use the Internet normally in step 340."

Examiner has read the claim limitations (Slemmer : Fig 1: item 130) access station in light of applicant's disclosure per [0033]-[0034], " A refers to an access station. An access station is used to connect a terminal device U to an IP-based infrastructure network, e.g. Intranet or Internet. It receives traffic from the IP network and delivers it to the correct terminal U, and, it receives traffic from terminals U and forwards it to the IP network..."

Giniger discloses locations of an edge devices per Col 2 lines 1-40, "The node device is, for example, *an edge device* located at a customer premises, or at an *Internet POP*, a network device located at an intermediate point in the Internet, or can be implemented in software on a computer at the customer premises. The node device includes a data storage containing cryptographic information including information that is private to the node device. The information that is private to the node device can include a private key of a public/private key pair known only to the node device, and can further include a certificate, such as a X.509 format certificate, which includes a public

key of the public/private key pair. The node device also includes *a tunneling communication service coupled to the network interface and is configured to maintain an encrypted communication tunnel with each of the multiple other node devices* using the cryptographic information."

As shown above, examiner relied on Giniger to interpret the edge device at the Internet POP, which is disclosed per the passage above. In response to applicant's arguments that accessing an internet in a trusted way between a user terminal via an untrusted access station, a review of the claim limitations recite, " disclose upon authentication of said terminal (U) and said ISP (P), said ISP performs the following: generating a session key ...". Slemmer was relied upon to disclose the authentication of said terminal (U) and the ISP (P). Giniger was relied upon to disclose the edge device, which is located at the ISP as stated above, distributing said session key, which per the passage, and creating a secure tunnel, per the claim limitations as described above.

Examiner has clearly pointed that out that the communication is secure from third party access station (Fig. 1 : item 130 , Slemmer). This reads on recited claim limitations, "that traffic transmitted between the terminal (U) and said Internet via said trusted network element (T) is secure from modification or eavesdropping by said third party access station (A)" Giniger discloses a router per trusted network element per Col 2 lines 32-40, "node device further includes a routing database for holding routing data and a router coupled to the tunneling communication service and to the routing database. The router is configured to accept communication from a first of the

computers ... and to pass the communication through the encrypted communication tunnel to the selected node device" The examiner asserts to have to read the claims in light of applicants disclosure per [0040; applicant's disclosure], " refers to a trusted network element. T is a router inside the Internet that P deems trustworthy to the extent that T does not provide A with means to snoop/insert/alter traffic from or to the terminal device U." Thus, examiner has read the claims in light of applicant's specification.

In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

To further add, Examiner has provided a pramie facie case of obviousness as the motivation in Giniger (Col 6 lines 14-22) was to provide comprehensive security to guarantee the safe transmission of mission critical data over public networks, and discloses that the control information exchanged between management server(s) and VPN devices is securely authenticated, encrypted, and protected from replay and other spoofing attacks.

3. Applicant argues: Claims 23, 26-27, 34 and 38 are not obvious over Slemmer, Giniger and Jensen

Response to 3.)

Please see the discussion above.

4. Applicant argues: Claims 33 and 41 are not obvious over Slemmer, Giniger and Bahl.

Response to 4.)

Please see the discussion above.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

Chirag Patel /C. R. P./

Examiner, Art Unit 2141

Conferees:

/Jason D Cardone/
Supervisory Patent Examiner, Art Unit 2145

Rupal Dharia

/Rupal D. Dharia/

Supervisory Patent Examiner, Art Unit 2141